REMARKS

Entry of the foregoing amendment is respectfully requested. This amendment is intended to place the claims in a more conventional format and eliminate the multiple dependency of the claims.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: James LaBarre
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: September 10, 2001

Attachment to Preliminary Amendment dated September 10, 2001

Marked-up Claims 1-7

1. (Amended) A countermeasure method against attacks by differential analysis in an electronic component implementing a secret key [(K)] cryptographic algorithm, the implementation of which comprises a number of successive calculation cycles [(T1, ... T16)] in order to supply, from first input data [(L0, R0)] applied to the first cycle [(T1)], final data [(L16, R16)] at the output of the last cycle [(T16) allowing the production of] to produce an encrypted message [(C)], each calculation cycle using calculation means [(TC)] for supplying an output data item [(S)] from an input data item [(E)], said calculation means [comprising the application of] performing the steps of:

applying a first random value [(u)] to the input data item [(E)] and to the output data item [(S)] in order to obtain [at the output] an unpredictable data item [($S\oplus u$), characterised in that the method comprises the use of means of] as an output, and

applying a second random value [(v)] to said first input data [(L0, R0), according to] by means of an EXCLUSIVE OR operation.

2. (Amended) A countermeasure method according to Claim 1, [characterised in that it also comprises the use of means] further including the step of applying the second random value [(v)] to the final data supplied by the last cycle [(T16), according to] by means of an EXCLUSIVE OR operation.

Attachment to Preliminary Amendment dated September 10, 2001

Marked-up Claims 1-7

3. (Amended) A countermeasure method according to [either one of the previous claims, characterised in that it comprises] claim 1 further including the step, at the end of each cycle, [the execution] of executing an additional operation [(CP(p(u))) in order] to eliminate said first random value [(u)] at the output of each cycle.

4. (Amended) A countermeasure method according to [any one of the previous claims, characterised in that it comprises the taking of] claim 1 wherein a new set of first and second random values [(u, v) and calculation of the calculation means (TC_M) used in each cycle] is selected for each new execution of the algorithm.

5. (Amended) A method according to Claim 4, [characterised in that] wherein said calculation means [(TC_M)] are calculated from first calculation means [(TC_0)] defining, for input data [(E)], corresponding output data [(S)], by applying the second random value [(v)] to said input data [($E\oplus e(v)$)] and applying the first random value [(u)] at least to said output data [($S\oplus u$)] of the first calculation means.

6. (Amended) A countermeasure method according to Claim 5, [characterised in that] wherein the calculation means [(TC_0, TC_M) are] comprise constants tables.

Attachment to Preliminary Amendment dated September 10, 2001

Marked-up Claims 1-7

7. (Amended) An electronic security component [implementing the] that implements a countermeasure method [against attacks by differential analysis comprising] for attacks against a secret key [(K)] cryptographic algorithm[, the implementation of which] by means of differential analysis, wherein said algorithm comprises a number of successive calculation cycles [(T1, ... T16)] in order to supply, from first input data [(L0, R0)] applied to the first cycle [(T1)], final data [(L16, R16)] at the output of the last cycle [(T16) allowing the production of] to produce an encrypted message [(C)], each calculation cycle using calculation means [(TC)] for supplying an output data item [(S)] from an input data item [(E)], said calculation means comprising the application of a first random value [(u)] to the input data item [(E)] and to the output data item [(S) in order] to obtain [at the output] an unpredictable output data item [($S\oplus u$), characterised in that], comprising first calculation means [(TC_0) are] fixed in a program memory [(1) of said component], second calculation means [(TC_M) used in each cycle being] that are calculated at each new execution of the algorithm and stored in working memory [(3)], and [in that it comprises] means [(4) of] for generating first and second random values [(u, v)] for calculating said second calculation means [(TC_M)].